

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-233460

(43)Date of publication of application : 10.09.1993

(51)Int.Cl. G06F 12/14
G06F 12/00

(21)Application number : 04-034764

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 21.02.1992

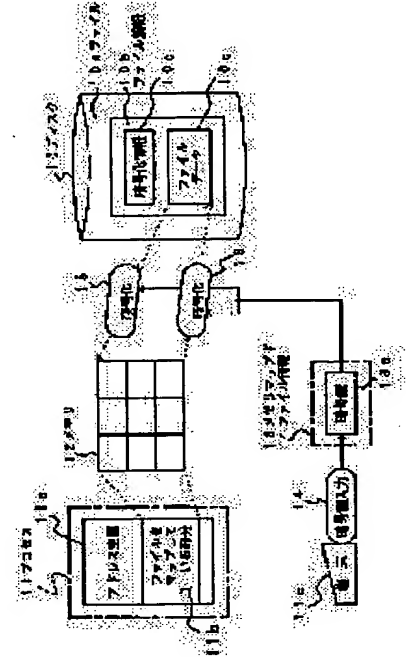
(72)Inventor : HIRAYAMA HIDEAKI

(54) FILE PROTECTION SYSTEM

(57)Abstract:

PURPOSE: To encipher a file placed on an external device at all times by providing means which decipher the data of an enciphered file among memory mapped files by using an enciphering key when the data are transferred from the external storage to a main memory and enciphers the data by using the enciphering key when the data are put back to the external storage.

CONSTITUTION: This system is equipped with a means which inputs the enciphering key from outside and records it as an enciphering key 13a in memory mapped file information 13, the deciphering means 15 which deciphers the data, block by block, by using the enciphering key 13a in the memory mapped file information 13 when the enciphered file data 10c are transferred from the disk 10 the main memory 12, and the enciphering means 16 which enciphers the file data on the main memory 12, block by block, by using the enciphering key 13a when the file data transferred to the main memory 12 are put back onto the disk 10.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平5-233460

(43) 公開日 平成5年(1993)9月10日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0 B	9293-5B		
12/00	5 3 7 H	7232-5B		

審査請求 未請求 請求項の数 2 (全 10 頁)

(21) 出願番号 特願平4-34764

(22) 出願日 平成4年(1992)2月21日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 平山 秀昭

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝総合研究所内

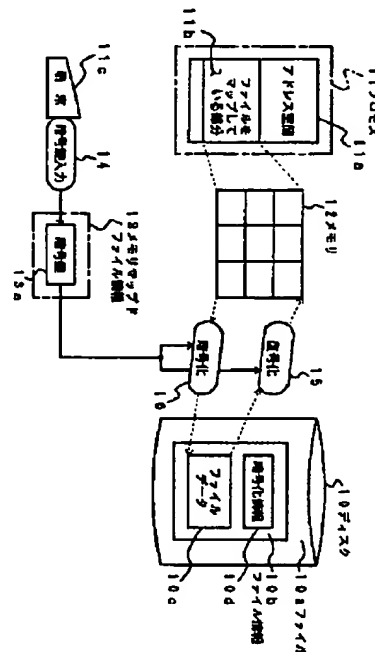
(74) 代理人 弁理士 鈴江 武彦

(54) 【発明の名称】 ファイル保護方式

(57) 【要約】

【目的】 本発明は、メモリマップドファイルに於いて、暗号化されたファイルのデータを外部記憶から主メモリに移す際に暗号鍵を用いて復号化し、そのデータを外部記憶へ戻す際に暗号鍵を用いて暗号化する手段を有して、外部記憶装置上に置かれたファイルを常に暗号化できることを最も主要な特徴とする。

【構成】 暗号鍵を外部より入力しメモリマップドファイル情報13中に暗号鍵13aとして記録する手段と、暗号化されたファイルデータ10cをディスク10から主メモリ12に移す際に、同データをメモリマップドファイル情報13中の暗号鍵13aを用いブロック単位で復号化する復号化手段15と、主メモリ12に移されたファイルデータをディスク10に戻す際に、主メモリ12上のファイルデータを暗号鍵13aを用いブロック単位で暗号化する暗号化手段16とを具備してなることを特徴とする。



【特許請求の範囲】

【請求項1】 外部記憶装置上のファイルをプロセスのアドレス空間上にマップし、プログラムからファイルを直接アクセスするメモリマップドファイルに於いて、主記憶上にマップするマップ対象ファイルが暗号化されているか否かを識別する手段と、

同手段で上記マップ対象ファイルが暗号化されていることを識別した際に外部より暗号鍵を入力し、対応ファイルがマップされている間、上記暗号鍵を保持する手段と、

上記暗号化されたファイルのデータを外部記憶装置から主記憶上に移す際に、同データを上記保持した暗号鍵を用いて復号化する手段と、

上記主記憶上のファイルのデータを外部記憶装置に戻す際に、同データを上記保持した暗号鍵を用いて暗号化する手段とを具備してなることを特徴とするファイル保護方式。

【請求項2】 ネットワークで接続されたりリモート電子計算機上のファイルをローカル電子計算機上のプロセスのアドレス空間上にマップし、プログラムからファイルを直接アクセスするメモリマップドファイルに於いて、上記マップの対象となるファイルが暗号化されているか否かを識別する手段と、

同手段で上記マップの対象となるファイルが暗号化されていることを識別した際に暗号鍵を外部より入力し、対応するファイルがマップされている間、上記暗号鍵を保持する手段と、

上記暗号化されたファイルのデータをリモート電子計算機からローカル電子計算機に移した後、同データを上記保持された暗号鍵を用いて復号化する手段と、

上記復号されたファイルのデータをローカル電子計算機からリモート電子計算機に戻す際に同データを上記保持された暗号鍵を用いて暗号化する手段とを具備してなることを特徴とするファイル保護方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、機密性の高いファイルを扱う電子計算機システムに適用して好適な、ファイルの情報漏洩を防ぐためのファイル保護方式に係り、特に、メモリマップドファイルの技術を用いて、機密性の高いファイルデータの高速アクセスとファイル保護を同時に実現可能にしたファイル保護方式に関する。

【0002】

【従来の技術】 近年、電子計算機システムは企業情報システムの構築に必須であり、かつ機密性の高い重要情報を保持する機会が益々増えている。社会構造が電子計算機への依存度を高めるにつれ、ハッカー、ウイルス等のコンピュータ犯罪が増えている。このため機密性の高いファイルの情報保護が、強く望まれている。その一方に於いて電子計算機はその用途を益々広げ、高速処理への

要求が止むことはない。

【0003】 そのため近年のメモリ価格の低下を利用して、ファイルをアドレス空間上に直接マップすることにより、高速なファイルアクセスを可能にする、メモリマップドファイルの技術が重視されている。

【0004】 機密性の高いファイルを保護するためには、ファイルを暗号化しておく必要があり、ファイルを高速にアクセスするためには、上記メモリマップドファイルの技術を利用する必要がある。

10 【0005】 しかし暗号化されたファイルを直接にメモリマップドファイルの技術を用いてアクセスすることはできず、暗号化されたファイルを格納した外部記憶上（ディスク上）にて一旦、復号化したファイルを作成し、そのファイルをメモリマップドファイルの技術を用いて、アクセスしなければならなかった。そのため結局のところ機密性の高いファイルが暗号化されない形でディスク上に存在してしまい、情報漏洩の危機に曝されてしまうという問題があった。

【0006】

20 【発明が解決しようとする課題】 上記したように従来のファイル保護方式は、ファイルを高速にアクセスするためのメモリマップドファイルの技術とは相容れないもので、従来のファイル保護方式をメモリマップドファイルの技術に適用することは困難であり、結局のところ機密性の高いファイルが暗号化されない形でディスク上に存在してしまい、情報漏洩の危機に曝されてしまうという問題があった。

30 【0007】 本発明は上記実情に鑑みなされたもので、機密性の高いファイルを暗号化したまま、復号化コピーを作ることなく、メモリマップドファイルの技術を用いて、ファイルを高速にアクセスすることにより、ファイルの保護と高速処理を同時に実現することができるファイル保護方式を提供することを目的とする。

【0008】

40 【課題を解決するための手段】 本発明のファイル保護方式は、外部記憶装置上のファイルをプロセスのアドレス空間上にマップし、プログラムからファイルを直接アクセスするメモリマップドファイルに於いて、主記憶上にマップするマップ対象ファイルが暗号化されているか否かを識別する手段と、同手段でマップ対象ファイルが暗号化されていることを識別した際に暗号鍵を外部より入力し、対応ファイルがマップされている間、上記暗号鍵を保持する手段と、上記暗号化されたファイルのデータを外部記憶装置から主記憶上に移す際に、上記保持した暗号鍵を用いて、上記データを上記各記憶装置間のデータ交換単位をもとに設定された所定のデータ量単位、例えばブロック単位で復号化する手段と、上記主記憶上のファイルのデータを外部記憶装置に戻す際に、上記保持した暗号鍵を用いて、上記データをブロック単位で暗号化

【0009】又、本発明のファイル保護方式は、ネットワークで接続されたりモート電子計算機上のファイルをローカル電子計算機上のプロセスのアドレス空間上にマップし、プログラムからファイルを直接アクセスするメモリマップドファイルに於いて、主記憶上にマップするファイルが暗号化されているか否かを識別する手段と、同手段でファイルが暗号化されていることを識別した際に暗号鍵を入力し、対応ファイルがマップされている間、上記暗号鍵を保持する手段と、上記暗号化されたファイルのデータをリモート電子計算機からローカル電子計算機に移した後、上記保持された暗号鍵を用いて上記データをブロック単位で復号化する手段と、上記復号化されたファイルのデータをローカル電子計算機からリモート電子計算機に戻す際に上記保持された暗号鍵を用いてデータをブロック単位で暗号化する手段とを具備したことを特徴とする。

【0010】

【作用】上記構成に於いて、暗号化されているファイルを主記憶上にマップする際は、外部から暗号鍵情報を入力し、メモリマップドファイル情報中に暗号鍵として記録する。その後、暗号化されたファイルのデータを外部記憶装置から主記憶上に移す際に、その暗号化されたファイルのデータを上記メモリマップドファイル情報中に含まれる暗号鍵を用いブロック単位で復号化する。又、主記憶上のファイルのデータを外部記憶装置に戻す際に、そのファイルのデータを上記暗号鍵を用いブロック単位で暗号化する。これにより外部記憶装置に格納されるファイルは常に暗号化されたファイルデータであり、従って、機密性の高いファイルを暗号化したまま、復号化コピーを作ることなく、メモリマップドファイルの技術を用いて、高速にアクセスすることができ、ファイルの保護と高速処理が同時に実現可能となる。

【0011】又、本発明のファイル保護方式に於いては、ネットワークで接続されたりモート電子計算機上のファイルをローカル電子計算機上のプロセスのアドレス空間上にマップして、ファイルを直接アクセスするメモリマップドファイル機構に於いても適用され、この際は、ローカル電子計算機の主記憶上にマップするファイルが暗号化されているとき、その暗号化されたファイルのデータをリモート電子計算機からローカル電子計算機に移した後に、外部より入力された暗号鍵を用いて上記データをブロック単位で復号化する。又、ローカル電子計算機の主記憶上のファイルのデータをローカル電子計算機からリモート電子計算機に戻す際は、そのファイルのデータを上記暗号鍵を用いブロック単位で暗号化し、リモート電子計算機に戻す。このように、暗号化されているデータは、ネットワークを経由して転送した後に復号化され、又、復号化されているデータは、ネットワークを経由して転送する前に暗号化されることにより、ネットワーク上を転送しているデータからの情報漏洩を防

ぐことができる。又、リモート電子計算機のファイルメモリ（外部記憶装置）上に於いては、常に暗号化されたファイルデータのみが格納される。従って、機密性の高いファイルを暗号化したまま、復号化コピーを作ることなく、メモリマップドファイルの技術を用いて、高速にアクセスすることができ、ファイルの保護と高速処理が同時に実現される。

【0012】

【実施例】以下図面を参照して本発明の一実施例を説明する。図1は本発明の一実施例の構成を示すブロック図である。ここでは、外部記憶装置となるディスク10上のファイル10aをプロセス11のアドレス空間11aの部分11bにマップしている。上記ファイル10aは、ファイル情報10bと、ファイルデータ10cより構成される。ファイル情報10b中には、ファイルデータ10cが暗号化されているか否かを示す暗号化情報10dが含まれる。

【0013】暗号化されているファイルを主メモリ12上にマップしようとした場合は、端末装置11cから暗号鍵を入力し、得られた暗号鍵情報をメモリマップドファイル情報13中に暗号鍵13aとして記録する。

【0014】尚、暗号鍵を入力する端末装置としては、ユーザの端末装置の他に、オペレータコンソール等も考えられる。また暗号鍵は、端末装置以外の装置から入力することも可能であり、例えばプログラム中に暗号鍵を埋め込む等も考えられる。

【0015】主メモリ12上にマップされたファイルをプロセス11がアクセスし、暗号化されているファイルデータ10cをディスク10から主メモリ12に移す場合には、その暗号化されているファイルデータ10cを上記メモリマップドファイル情報13中の暗号鍵13aを用いてブロック単位で復号化する。

【0016】即ち、主メモリ12上にマップするファイルのデータが暗号化されている（マップ対象ファイルのファイル情報10bに含まれる暗号化情報10dが、ファイル情報10bの暗号化されていることを示している）際は、その暗号化されたファイルデータ10cをディスク10から主メモリ12に移す際に、そのデータが、復号化手段15により、メモリマップドファイル情報13中の暗号鍵13aを用いブロック単位で復号化される。

【0017】また逆に、ディスク10から主メモリ12に移されていた復号化されたデータを、再びディスク10に戻す場合も同データを上記暗号鍵13aを用いてブロック単位で暗号化する。

【0018】即ち、上記復号化手段15により復号化され主メモリ12に移されたファイルデータをディスク10に戻す際は、主メモリ12上のファイルデータが暗号化手段16により上記暗号鍵13aを用いてブロック単位で暗号化される。図2は上記図1に示す実施例に於い

5

て、暗号化されているファイルを主メモリ12上にマッピングするマッピング処理の流れを示すフローチャートである。

【0019】図2に於いて、A1は主メモリ12上にマップするファイルが暗号化されているか否かを調べる判断ステップである。ここで暗号化されていることを判断すると、ステップA2、A3の処理を行ってからステップA4の処理を行なう。また、暗号化されていない場合は、ステップA2、A3の処理は行わず、ステップA4の処理を行なう。

【0020】A2は暗号鍵13aを入力する処理ステップ、A3は入力された暗号鍵13aをメモリマップドファイル情報13中に記録する処理ステップである。A4は通常のメモリマップドファイルのマッピング処理を行う処理ステップである。

【0021】図3は上記図1に示す実施例に於いて、主メモリ12上にマッピングされた暗号化ファイルのデータをディスク10から主メモリ12上に移す処理（メモリマップドファイルのページイン処理）の流れを示すフローチャートである。

【0022】図3に於いて、B1は主メモリ12上にマップされたファイルのページをディスク10から主メモリ12に移すステップである。B2は主メモリ12上にマップされたファイルのデータが暗号化されているか否かを調べる判断ステップである。

【0023】ここで、上記マップされたファイルのデータが暗号化されているときは、ステップB3の処理を行ってからステップB4の処理を行なう。又、上記マップされたファイルのデータが暗号化されていないときは、ステップB3の処理は行わずにステップB4の処理を行なう。

【0024】B3はディスク10から主メモリ12に移すページ中のデータを暗号鍵13aを用いて復号化する処理ステップであり、B4は通常のメモリマップドファイルのページイン処理を行なう処理ステップである。

【0025】図4は上記図1に示す実施例に於いて、主メモリ12上にマッピングされている暗号化ファイルのデータを主メモリ12からディスク10に戻す処理（メモリマップドファイルのページアウト処理）の流れを説明するフローチャートである。図4に於いて、C1は主メモリ12上にマップされているファイルが暗号化するファイルのデータであるか否かを調べる処理ステップである。

【0026】ここで暗号化するファイルのデータであるときは、ステップC2の処理を行ってからステップC3、C4の処理を行なう。又、暗号化しないファイルのデータであるときはステップC2の処理を行わずにステップC3、C4の処理を行なう。

【0027】C2は主メモリ12からディスク10に戻すページ中のデータを暗号鍵13aを用いて暗号化する

6

処理ステップであり、C3は主メモリ12上にマップされたファイルのページをディスク10に戻すステップである。C4は通常のメモリマップドファイルのページアウト処理を行なう処理ステップである。

【0028】上記図1乃至図4に示す実施例に於いて、ディスク10上の暗号化されているファイルを主メモリ12上にマップする際は、端末装置11cから暗号鍵を入力し、その入力された暗号鍵情報をメモリマップドファイル情報13中に暗号鍵13aとして記録する。

10 【0029】即ち、この際の暗号化されているファイルを主メモリ12上にマッピングするマッピング処理では、主メモリ12上にマップするファイルが暗号化されているか否かを調べる（図2ステップA1）。

【0030】この際、主メモリ12上にマップするファイルのファイル情報10bに含まれる暗号化情報10dは、該当ファイル情報10bが暗号化されているか否かを示している。

20 【0031】ここで、主メモリ12上にマップするファイルのデータが暗号化されている際は、暗号鍵を入力する処理で入力された暗号鍵情報を暗号鍵13aとしてメモリマップドファイル情報13中に記録（図2ステップA2、A3）した後、通常のメモリマップドファイルのマッピング処理を行なう（図2ステップA4）。

【0032】又、主メモリ12上にマップするファイルのデータが暗号化されていない際は、上記暗号鍵の処理（図2ステップA2、A3）を行わずに、通常のメモリマップドファイルのマッピング処理を行なう（図2ステップA4）。

30 【0033】上記マッピング処理により主メモリ上にマップされたファイルをプロセス11がアクセスし、そのファイルのデータをディスク10から主メモリ12に移す際は、該当ファイルデータ10cが暗号化されていれば、その暗号化されているファイルデータ10cが上記メモリマップドファイル情報13中の暗号鍵13aを用いて復号化される。

【0034】即ち、ディスク10上のファイルデータを主メモリ12に移す際は、ディスク10より読出されるファイルのデータが暗号化されているか否かが判断される（図3ステップB1）。

40 【0035】ここで、主メモリ上にマップされたファイルのデータが暗号化されている際は、その暗号化されたファイルデータ10cをディスク10から主メモリ12上に移す際に、そのデータが、復号化手段15により、メモリマップドファイル情報13中の暗号鍵13aを用いブロック単位で復号化され（図3ステップB2、B3）、その復号化処理を介して、メモリマップドファイルのページイン処理が行なわれる（図3ステップB4）。

50 【0036】次に、ディスク10から主メモリ12上に移されている、復号化されたデータをディスク10に戻

7

す場合も、その復号化されたデータが上記暗号鍵13aを用いて暗号化される。

【0037】即ち、主メモリ12のファイルデータをディスク10に戻す際は、主メモリ12上にマップされているファイルが暗号化するファイルのデータであるか否かが判断される(図4ステップC1)。

【0038】ここで、暗号化するファイルのデータであるときは、主メモリ12からディスク10に戻すページ中のデータが暗号化手段16により暗号鍵13aを用いて暗号化され(図4ステップC2、C3)、その暗号化処理を介在して、メモリマップドファイルのページアウト処理が行なわれる(図4ステップC4)。

【0039】このようなファイルの処理制御により、暗号化されたファイルはディスク10上では復号化されることがなく、従って「トロイの木馬」のような手法(ファイルとして見えても真のデータは隠されている状態)により、ファイル自体が不正コピー等により盗難されたとしても、暗号鍵の盗難がない限り、機密情報の漏洩を防止することができる。

【0040】また主メモリ12上にマップされたファイルのページイン/ページアウト処理が頻発すると、ファイルデータの暗号化/復号化のオーバーヘッドが増加するが、近年はメモリ価格が低下しているので、大容量のメモリを使用することにより、この問題は解消される。図5は本発明の他の実施例を示すブロック図である。

【0041】ここでは、リモートノード28上のディスク20に格納されたファイル20aを、ローカルノード27上のプロセス21のアドレス空間21aの部分21bにマップする例を示している。この際、上記ファイル20aはファイル情報20bとファイルデータ20cより構成されるものとする。ファイル情報20b中には暗号化情報20dが含まれていて、ファイルデータ20cが暗号化されているか否かを示している。

【0042】暗号化されているファイルをメモリ22上にマップしようとした場合は、端末装置21cに対して暗号鍵を要求し、得られた暗号鍵情報をメモリマップドファイル情報23中に、暗号鍵23aとして記録する。29はローカルノード27とリモートノード28が通信を行なうためのネットワークである。

【0043】メモリ22上にマップされたファイルをプロセス21がアクセスし、暗号化されているファイルデータをネットワーク29を経由して、リモートノード28のディスク20からローカルノード27のメモリ22に移す場合には、ファイルデータ20cがネットワーク29を経由してローカルノード27に送られた後に、復号化手段25により暗号鍵23aを用いてブロック単位で復号化される。

【0044】また、これとは逆に、リモートノード28のディスク20からローカルノード27のメモリ22に移されていたデータをネットワーク29を経由して再び

8

リモートノード28のディスク20に戻す場合には、そのファイルデータをネットワーク29を経由してリモートノード28に送る際に、暗号化手段26により暗号鍵23aを用いてブロック単位で再び暗号化される。

【0045】このように、暗号化されているデータは、ネットワーク29を経由して転送した後に復号化され、又、復号化されているデータは、ネットワーク29を経由して転送する前に暗号化されることにより、ネットワーク29上を転送しているデータからの情報漏洩を防ぐことができる。

【0046】

【発明の効果】以上詳記したように本発明のファイル保護方式によれば、外部記憶装置上のファイルをプロセスのアドレス空間上にマップし、プログラムからファイルを直接アクセスするメモリマップドファイルに於いて、主記憶上にマップするマップ対象ファイルが暗号化されているか否かを識別する手段と、同手段でマップ対象ファイルが暗号化されていることを識別した際に暗号鍵を外部より入力し、対応ファイルがマップされている間、上記暗号鍵を保持する手段と、上記暗号化されたファイルのデータを外部記憶装置から主記憶上に移す際に、上記保持した暗号鍵を用いて、上記データを所定のデータ転送単位(例えばブロック単位)で復号化する手段と、上記主記憶上のファイルのデータを外部記憶装置に戻す際に、上記保持した暗号鍵を用いて、上記データをブロック単位で暗号化する手段とを具備してなる構成としたことにより、機密性の高いファイルを暗号化したまま、復号化コピーを作ることなく、メモリマップドファイルの技術を用いて、高速にアクセスすることができ、ファイルの保護と高速処理を同時に実現できる。

【0047】又、本発明のファイル保護方式によれば、ネットワークで接続されたりリモート電子計算機上のファイルをローカル電子計算機上のプロセスのアドレス空間上にマップし、プログラムからファイルを直接アクセスするメモリマップドファイルに於いて、主記憶上にマップするファイルが暗号化されているか否かを識別する手段と、同手段でファイルが暗号化されていることを識別した際に暗号鍵を入力し、対応ファイルがマップされている間、上記暗号鍵を保持する手段と、上記暗号化されたファイルのデータをリモート電子計算機からローカル電子計算機に移した後、上記保持された暗号鍵を用いて上記データをブロック単位で復号化する手段と、上記復号されたファイルのデータをローカル電子計算機からリモート電子計算機に戻す際に上記保持された暗号鍵を用いてデータをブロック単位で暗号化する手段とを具備してなる構成としたことにより、暗号化されているデータは、ネットワークを経由して転送した後に復号化され、又、復号化されているデータは、ネットワークを経由して転送する前に暗号化されることから、ネットワーク上を転送しているデータからの情報漏洩を防ぐことができ

る。又、リモート電子計算機のファイルメモリ（外部記憶装置）上に於いては、常に暗号化されたファイルデータのみが格納されることから、機密性の高いファイルを暗号化したまま、復号化コピーを作ることなく、メモリマップドファイルの技術を用いて、高速にアクセスすることができ、ファイルの保護と高速処理が同時に実現できる。

【図面の簡単な説明】

【図1】本発明の一実施例の構成を示すブロック図。

【図2】図1の実施例に於いて、暗号化されたファイルをメモリ上にマッピングする処理を説明するためのフローチャート。

【図3】図1の実施例に於いて、メモリ上にマップされた暗号化対象ファイル中のデータをディスクからメモリに移す処理を説明するためのフローチャート。

【図4】図1の実施例に於いて、メモリ上にマップされた暗号化ファイル中のデータを、メモリからディスクに

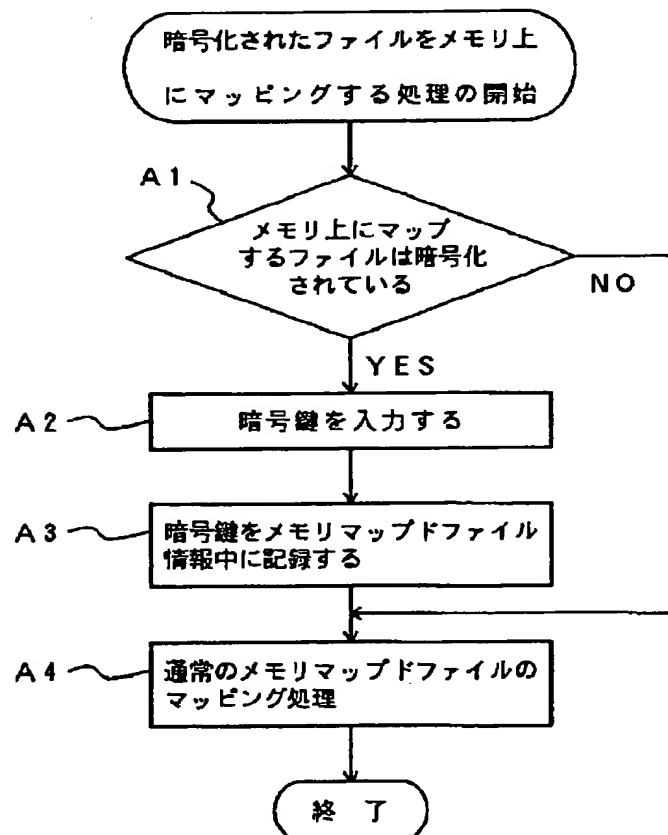
戻す処理を説明するためのフローチャート。

【図5】本発明の他の実施例の構成を示すブロック図。

【符号の説明】

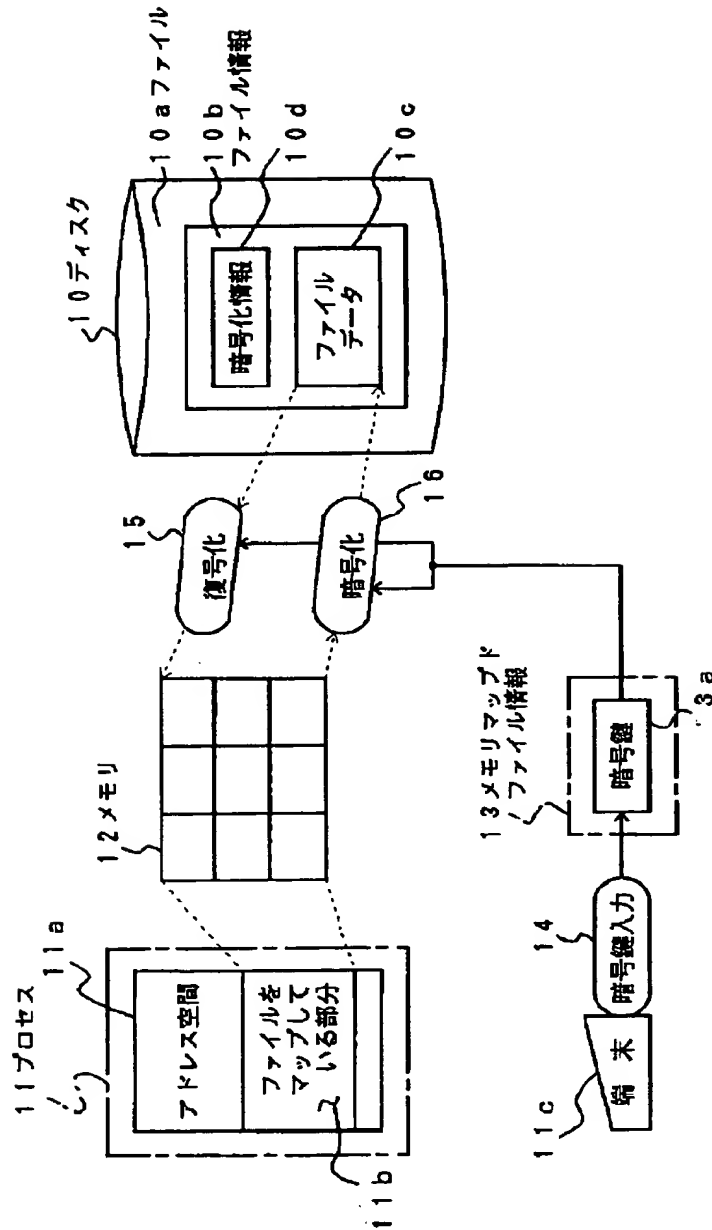
10…ディスク、10a…ファイル、10b…ファイル情報、10c…ファイルデータ、10d…暗号化情報、11…プロセス、11a…アドレス空間、11b…ファイルをマップしている部分、11c…端末装置、12…メモリ、13…メモリマップドファイル情報、13a…暗号鍵、14…暗号鍵入力手段、15…復号化手段、16…暗号化手段、20…ディスク、20a…ファイル、20b…ファイル情報、20c…ファイルデータ、20d…暗号化情報、21…プロセス、21a…アドレス空間、21b…ファイルをマップしている部分、21c…端末装置、22…メモリ、23…メモリマップドファイル情報、23a…暗号鍵、24…暗号鍵入力手段、25…復号化手段、26…暗号化手段、27…ローカルノード、28…リモートノード、29…ネットワーク。

【図2】

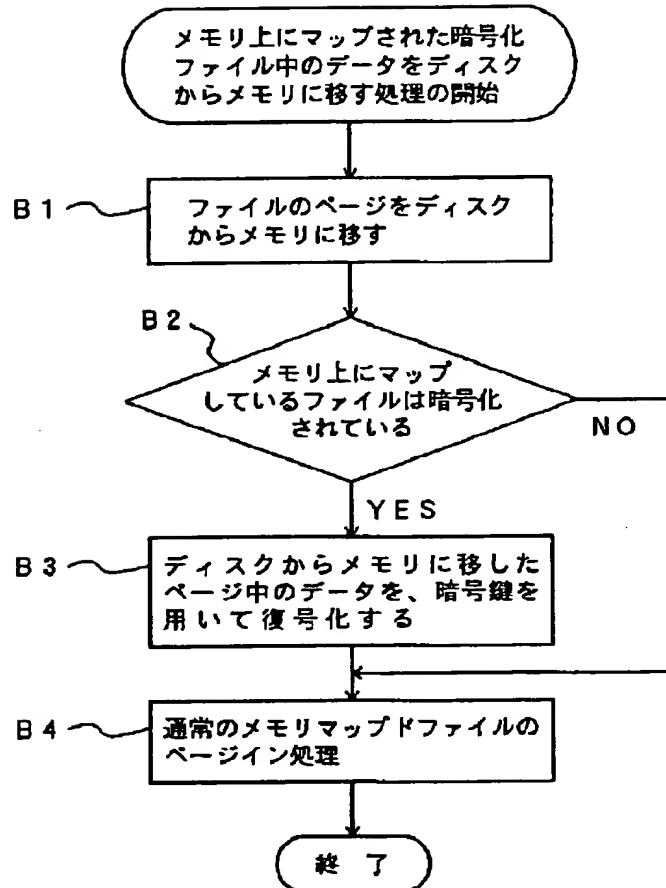


(7)

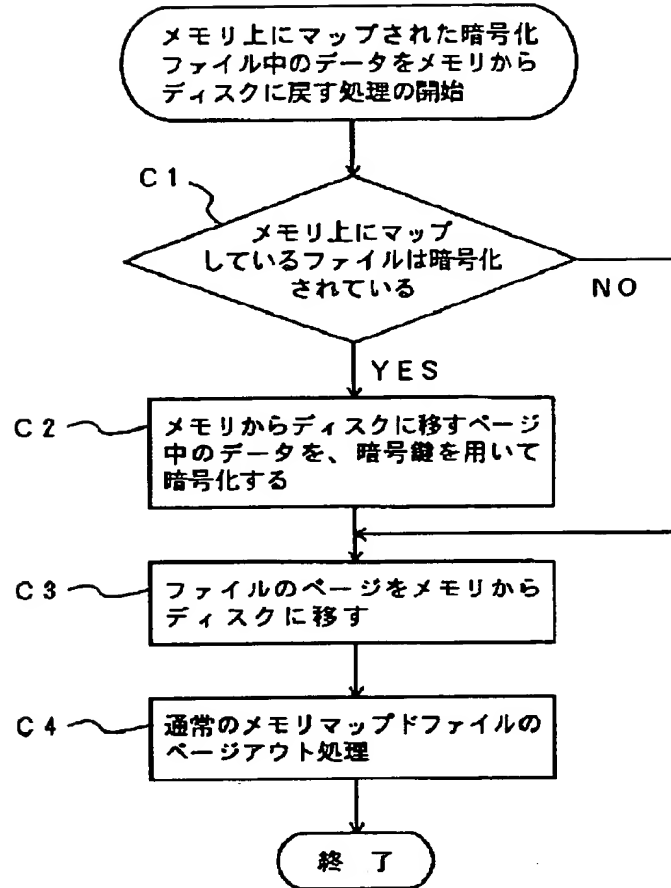
【図1】



【図3】



【図4】



【図5】

